



In the Claims:

Please cancel claim 11, without prejudice, and amend claims 1 and 3-10 as

follows:

1. (Currently Amended) A private data protection distribution method, comprising:

receiving encrypted private data;

receiving an encrypted private data use license which describes a decryption key for decrypting the encrypted private data, and a use condition of the encrypted private data;

decrypting the decryption key and the private data use license;

determining whether or not a use purpose of the encrypted private data matches the use condition described in the private data use license; and

decrypting the encrypted private data by using the decrypted decryption key only if the use purpose of the encrypted private data matches the use condition.

2. (Original) The private data protection distribution method according to claim 1, wherein

the decryption key and the private data use license are encrypted and decrypted by using a DRM authentication technology.

3. (Currently Amended)

The private data protection distribution

method according to claim 2, wherein

a mechanism for decrypting the private data use license by using a DRM

authentication technology is implemented as a ~~TRM~~Tamper Resistant Module (TRM).

4. (Currently Amended)

The private data protection distribution

method according to claim 1, wherein

the use condition of the private data use license includes at least any of an

~~expiry~~expire date, a number of available times, a use purpose, and a number of move times of
the private data use license.

5. (Currently Amended)

The private data protection distribution

method according to claim 4, wherein

the use purpose includes a restriction on an application which uses the

encrypted private data.

6. (Currently Amended)

The private data protection distribution

method according to claim 1, further comprising:

receiving the encrypted private data, and the encrypted private data use license

which describes the decryption key for decrypting the encrypted private data, and the use
condition of the encrypted private data from a plurality of information entities;

creating a name list license by concatenating a plurality of private data use licenses which have the same conditions; and

creating a name list by concatenating encrypted private data which correspond to the private use licenses used to create the name list license.

7. (Currently Amended) The private data protection distribution method according to claim 6, wherein

the encrypted private data can be decrypted with a decryption key possessed by an information entity that transmits the encrypted private data.

8. (Currently Amended) The private data protection distribution method according to claim 6, wherein

if the encrypted private data is provided to a different information device, at least any one of a name, a type, a use purpose, ~~and~~ an inquiry destination of an organization which manages a different information device to which the encrypted private data is provided, and a provided item list of a private data database is created for each information entity, and is disclosed to a corresponding information entity depending on need.

9. (Currently Amended) The private data protection distribution method according to claim 8, further comprising:

receiving corrected contents if a correction is made to at least one of the encrypted private data, and the private data use license which describes the decryption key for decrypting the encrypted private data, and the use condition of the encrypted private data; and

transmitting the corrected contents to a different information device to secure a sameness of the encrypted private data and the private data use license.

10. (Currently Amended) A computer readable storage medium storing
a A private data protection distribution program for causing a computer to execute a process, the process comprising:

receiving encrypted private data;

receiving an encrypted private data use license which describes a decryption key for decrypting the encrypted private data, and a use condition of the encrypted private data;

decrypting the decryption key and the private data use license;

determining whether or not a use purpose of the encrypted private data matches the use condition described in the private data use license; and

decrypting the encrypted private data by using the decrypted decryption key only if the use purpose of the encrypted private data matches the use condition.

11. (Cancelled)